Transkrypcja cyklu audycji „Bezpieczne Złotówki” realizowanego w rozgłośni Radia Pogoda we współpracy z Fundacją THINK! To sześć odcinków rozmów z ekspertami o tym, jak chronić pieniądze przed cyberoszustami.

Odcinek 1. Gość – Marcin Maj

Prowadzący: Wystarczy chwila uwagi, by stracić dostęp do konta w mediach społecznościowych. Oszuści w naszym imieniu mogą na przykład wysyłać fałszywe wiadomości, a nawet fałszywe prośby o przelew do bliskich. Co zrobić, aby do tego nie dopuścić? Podpowiada Marcin Maj, analityk OSINT, specjalista do spraw ochrony danych i redaktor niebezpiecznik.pl. Po co przestępcom dostęp do naszego konta na Facebooku lub Instagramie?

Marcin Maj: Przejęcia kont w social mediach rzeczywiście mogą służyć do kradzieży pieniędzy i może do tego dojść na trzy sposoby. Po pierwsze, przestępcy mogą użyć konta po to, aby podszywając się pod nas, na przykład na Facebooku, skontaktować się z naszymi znajomymi i poprosić ich o jakiegoś rodzaju przysługę lub pożyczkę. Może to być kliknięcie w jakiś link, przekazanie kodu BLIK. Tutaj scenariusze są różne, ale skończy się to ostatecznie wyłudzeniem pieniędzy od naszych znajomych niejako w naszym imieniu. Poza tym dostęp do konta może być użyty do pozyskania wrażliwych danych osobowych, które zostaną dalej wykorzystane w oszustwie. Zdarza się również, że oszuści będą żądać okupu w zamian za odzyskanie dostępu do konta.

Prowadzący: Co może świadczyć o tym, że ktoś włamał się na nasze konto? Jak to rozpoznać?

Marcin Maj: Jeśli nagle nie możemy się zalogować na swoje konto albo doszło do jakichś istotnych zmian na koncie, o których nie mieliśmy pojęcia, to zdecydowanie jest to sygnał, że ktoś się na nie włamał. Niestety znamy również sytuacje, kiedy oszuści celowo ukrywają swoją obecność na koncie. Przykładowo potrafią wysłać wiadomość do znajomego w naszym imieniu, a zaraz po tym ją skasować, abyśmy nie wiedzieli, że jakaś korespondencja została wymieniona.

Prowadzący: Jakie kroki powinniśmy podjąć natychmiast po wykryciu takiego włamania?

Marcin Maj: Jeśli mamy choćby cień podejrzenia, że obca osoba dostała się na nasze konto, powinniśmy przede wszystkim zresetować hasło, aby odebrać tej osobie możliwość dalszego logowania się. Powinno dojść do wylogowania się ze wszystkich aktywnie zalogowanych sesji. Zmieńmy hasło, przejrzyjmy wszystkie dokonane czynności i ewentualnie rozważmy wprowadzenie na konto dodatkowych zabezpieczeń, jeśli dotąd ich nie włączyliśmy.

Prowadzący: Jak zabezpieczyć konto, aby utrudnić działanie oszustowi?

Marcin Maj: Podstawowym zabezpieczeniem konta jest hasło, które powinno być nie tylko mocne, ale przede wszystkim unikalne. Czyli nie powinno być to hasło używane w social mediach i jeszcze gdzie indziej, dlatego że hasła z różnych miejsc wyciekają. Niech to będzie jedno hasło do jednego konta. Poza tym współczesne serwisy dają nam możliwość

włączenia logowania dwuskładnikowego, czyli takiego, które jest dodatkowo potwierdzane kodem z SMS-a lub aplikacji. Włączmy to zabezpieczenie. Najwyższy poziom bezpieczeństwa dają tak zwane klucze U2F, czyli specjalne urządzenia USB do potwierdzania swoich logowań, które można kupić i spiąć ze swoim kontem.

Lektor: Partnerem cyklu jest Fundacja Rozwoju Społeczeństwa Wiedzy THINK!, organizator kampanii edukacyjnej „Bezpieczne złotówki". Kampania „Bezpieczne złotówki" finansowana jest ze środków Funduszu Edukacji Finansowej, którego dysponentem jest Minister Finansów. Kampania wspiera realizację Krajowej Strategii Edukacji Finansowej.

Odcinek 2. Gość – Karol Bojke

Prowadzący: Hasło do konta w banku czy numer PIN karty płatniczej – to dane, o które powinniśmy dbać szczególnie. Nie chcemy przecież, aby trafiły w ręce cyfrowych oszustów, którzy czyhają na nasze pieniądze. O tym, jak chronić dostęp do naszych cyfrowych zasobów, opowie Karol Bojke, ekspert CERT Polska. Gdzie na pewno nie powinniśmy przechowywać naszych haseł, aby nie ryzykować, że trafią w ręce cyfrowych oszustów?

Karol Bojke: Większość z nas ma świadomość, że trzymanie haseł zapisanych na karteczce przy monitorze albo pod klawiaturą jest złym pomysłem. Podobnie jest z formą cyfrową. Na komputerze nie zapisujmy haseł w notatniku, w dokumentach pakietu Office czy w wiadomości do kogoś bliskiego. Jeśli przestępcy uzyskają dostęp do naszego urządzenia, to na pewno sprawdzą właśnie te miejsca.

Prowadzący: Czy najważniejsze hasła możemy przechowywać na naszym komputerze?

Karol Bojke: Możemy, a nawet jest to wskazane pod warunkiem, że będziemy to robić z głową. Korzystajmy z menedżerów haseł. Są to aplikacje i usługi, które nie tylko pomogą nam bezpiecznie przechowywać wiele haseł, ale też sprawią, że nie musimy ich znać na pamięć. Podpowiedzą nam właściwe hasło podczas logowania i wygenerują nowe, gdy rejestrujemy się w nowym miejscu. A to bardzo ważne, żeby mieć unikalne hasła do różnych portali. Kluczowe jest to, żeby dostęp do tej aplikacji, do naszego sejfu z hasłami, był dobrze strzeżony. Zadbajmy o dwuskładnikową weryfikację. Poza hasłem do sejfu włączmy też uwierzytelnianie kodem z SMS-a lub z dedykowanej aplikacji. A jeśli nigdy tego nie robiliśmy, warto poprosić kogoś bliskiego o pomoc.

Prowadzący: A co z tradycyjnymi sposobami? Na przykład papierowym notatnikiem.

Karol Bojke: Wszystko sprowadza się do tego, jak skutecznie możemy chronić swoje hasła. Unikajmy zapisywania ich w swoim codziennym kalendarzu, który czasem zostawiamy bez opieki w widocznym miejscu. Jeśli chcemy je przechowywać w formie papierowej, poświęćmy im oddzielny zeszyt trzymany w zamykanej szafce, do której klucz mamy w innym miejscu, najlepiej przy sobie. Lokalizacji zeszytu nie zdradzajmy nikomu obcemu, bo choć cyberprzestępcy nie włamią nam się na papier, to zwykli złodzieje już mogą.

Prowadzący: Gdzie i w jaki sposób powinniśmy dokonać zgłoszenia, jeśli podejrzewamy, że ktoś mógł wykraść nasze hasła?

Karol Bojke: Zanim pomyślimy o zgłoszeniu, zadbajmy o bezpieczeństwo swoich kont. Upewnijmy się, że nikt nie zdążył się na nie zalogować, a jeśli tak – zakończmy wszystkie aktywne sesje. Można to zrobić w ustawieniach konta. Następnie zmieńmy hasło i w przypadku bankowości elektronicznej poinformujmy również bank o możliwych próbach wykonania operacji w naszym imieniu. Gdy podejrzewamy, że ktoś mógł wyłudzić hasło, poinformujmy policję. A jeśli działo się to za pośrednictwem internetu, to także zespół CERT Polska na stronie incydent.cert.pl lub w aplikacji mObywatel w usłudze „Bezpiecznie w sieci".

Odcinek 3. Gość – Monika Przestrzelska

Prowadzący: Oszuści cyfrowi nie zawsze atakują z rozmachem. Często próbują wyłudzić drobne kwoty, licząc na to, że poszkodowana osoba nie zgłosi tego na policję. Tymczasem każda taka próba może być częścią większego procederu, a sumy ukradzionych złotówek mogą sięgać setek tysięcy. Aspirant Monika Przestrzelska z policyjnego Centralnego Biura Zwalczania Cyberprzestępczości opowiada o tym, dlaczego zawsze warto reagować na oszustwa. Dlaczego tak niewielu seniorów zgłasza oszustwa na policję?

Aspirant Monika Przestrzelska: Zacznijmy od tego, że seniorzy to grupa społeczna, która wbrew pozorom jest coraz bardziej świadoma zagrożeń. Docierają do nich różnego rodzaju kampanie prowadzone między innymi przez fundacje, banki, NASK czy też policję. Kampanie te uświadamiają o czyhających zagrożeniach. Mamy świadomość tego, że część osób może nie do końca zdawać sobie sprawę z tego, że po prostu została oszukana. Ale też wśród każdej grupy społecznej – czy to wśród młodzieży, dorosłych, czy właśnie seniorów – znajdują się osoby, które nie zgłaszają się na policję po prostu ze wstydu. Wstydzą się tego, że dały się oszukać. A prawda jest taka, że to nie oni powinni się wstydzić.

Prowadzący: Czy warto zgłaszać każdą próbę oszustwa, nawet jeśli chodzi o kradzież drobnej kwoty?

Aspirant Monika Przestrzelska: Jak najbardziej. Warto zgłaszać każdą próbę oszustwa. Policjanci każdego dnia reagują na różnego rodzaju przestępstwa i wykroczenia, ale też próbują im zapobiegać. Zgłaszanie próby oszustwa może pomóc w zapobieganiu oszukaniu innych osób. Wszystkim nam zależy na bezpieczeństwie, a zgłaszając próbę oszustwa, przyczyniamy się do jego poprawy.

Prowadzący: Jak wygląda procedura takiego zgłoszenia? Czy to skomplikowane?

Aspirant Monika Przestrzelska: Nie ma niczego skomplikowanego w zgłoszeniu oszustwa. Przychodząc na policję, przygotujmy się jednak do złożenia zawiadomienia. Przykładowo, w sytuacji, gdy oszuści przesłali nam fałszywego SMS-a, miejmy przy sobie telefon i wszystkie istotne w sprawie materiały – czy to zrzuty ekranu, czy też gotowe wydruki. Jeśli nie umiemy

zrobić zrzutu ekranu lub nie mamy możliwości wydrukowania materiałów, po prostu weźmy ze sobą telefon. Zabierzmy też dokument potwierdzający naszą tożsamość.

Prowadzący: Podsumujmy, w jaki sposób możemy zgłosić kradzież i oszustwo.

Aspirant Monika Przestrzelska: Jeżeli oszuści ukradli pieniądze z konta, to pierwszym krokiem, jaki powinniśmy wykonać, jest skontaktowanie się z bankiem w celu zablokowania dalszych transakcji. Tu czas gra rolę – im szybciej to zrobimy, tym lepiej. Kolejnym krokiem jest skontaktowanie się z policją. Możemy to zrobić od razu telefonicznie, uzyskując informacje o następnych krokach. Na kolejnym etapie będziemy musieli udać się do najbliższej jednostki policji w celu złożenia zawiadomienia osobiście.

Odcinek 4. Gość – Piotr Mieczkowski

Prowadzący: Choć w internecie czyhają na nas zagrożenia, nie znaczy to, że powinniśmy rezygnować z wygód, jakie oferuje nam cyfryzacja. Jak korzystać z cyfrowych narzędzi bez lęku, ale z rozsądkiem – radzi Piotr Mieczkowski z fundacji Digital Poland. Jak bezpiecznie korzystać z aplikacji bankowych i płatności mobilnych?

Piotr Mieczkowski: Przede wszystkim pobierajmy aplikacje bankowe z oficjalnych źródeł, takich jak Google Play czy App Store. Nie instalujmy aplikacji z niezaufanych źródeł. Używajmy unikalnych i silnych haseł. Jeśli używamy kodu PIN, to tylko i wyłącznie w aplikacji bankowej – nie używajmy go w innym miejscu. Regularnie aktualizujmy aplikacje i system naszego telefonu, by chronić się przed lukami w zabezpieczeniach.

Prowadzący: Na co powinniśmy zwrócić uwagę, gdy korzystamy z publicznego dostępu do internetu? Na przykład na dworcu albo w kawiarni.

Piotr Mieczkowski: Wchodząc do kawiarni czy na dworzec, zwróćmy uwagę, gdzie są kamery i starajmy się nie korzystać z bankowości online, siedząc bezpośrednio pod nimi, gdyż nasze dane mogą zostać odczytane przez lokalny monitoring. Po drugie, raczej korzystajmy z własnego internetu, a jeśli musimy skorzystać z publicznego Wi-Fi, użyjmy aplikacji VPN, która pozwala szyfrować dane. Zwracajmy też uwagę, czy sieć Wi-Fi wymaga hasła – te, które go wymagają, są zazwyczaj bezpieczniejsze. Mimo to nie polecam kawiarni do robienia przelewów, ponieważ ktoś mógłby stworzyć fałszywy punkt dostępowy.

Prowadzący: Nie dać się oszukać, ale też nie panikować. O jakich trzech rzeczach powinien pamiętać aktywny cyfrowo senior?

Piotr Mieczkowski: Po pierwsze, pamiętajmy, że jest bardzo dużo fałszywych kampanii – SMS-ów, wiadomości czy reklam. W związku z tym nie klikajmy w podejrzane linki ani nie podawajmy danych osobowych. Sprawdzajmy dwa razy adres WWW lub e-mail, czy aby na pewno pochodzi od zaufanego źródła. Po drugie, aktualizujmy oprogramowanie i używajmy silnych haseł. Po trzecie, edukujmy się, podnośmy kompetencje cyfrowe i cieszmy się światem cyfrowym.

Odcinek 5. Gość – Joanna Rudzińska-Wojciechowska

Prowadzący: Silne emocje, presja czasu, podszywanie się pod bliskich – to tylko niektóre techniki, jakie stosują oszuści, by nami manipulować. Dlaczego wciąż działają i jak się przed nimi bronić? O tym opowie dr Joanna Rudzińska-Wojciechowska, psycholog z Akademii Leona Koźmińskiego. Na jakie sztuczki cyfrowych oszustów powinniśmy być szczególnie wyczuleni?

Joanna Rudzińska-Wojciechowska: Przede wszystkim naszą czujność powinny wzbudzić wszystkie sytuacje, kiedy ktoś wywiera na nas presję czasu. Oszuści celowo tworzą poczucie, że trzeba działać natychmiast. Kiedy słyszymy, że za kilka minut zablokowane zostanie nasze konto albo że mamy ostatnie minuty, żeby skorzystać z jakiejś okazji, zaczynamy działać impulsywnie. A w stresie i pośpiechu podejmujemy kiepskie decyzje. Zaniepokoić nas powinno również to, gdy ktoś stara się bardzo szybko zbudować z nami bliskość. Oszuści potrafią być niezwykle cierpliwi i mili, a wszystko po to, żebyśmy stali się mniej czujni i mniej skłonni do zadawania pytań.

Prowadzący: Dlaczego ich metody, choć często znane, wciąż bywają skuteczne?

Joanna Rudzińska-Wojciechowska: Jedną z przyczyn jest to, że przestępcy doskonale opanowali sposoby wytrącenia nas z rozsądnego trybu funkcjonowania. Wywołują w nas silne emocje: strach lub ekscytację, najlepiej połączone z presją czasu. W takim stanie nie mamy łatwego dostępu do naszej wiedzy. Drugi sposób to uśpienie czujności poprzez liczne zapewnienia, że z ofertą jest wszystko w porządku. Ponadto paradoksalnie przekonanie, że mamy dużą wiedzę i nas to zagrożenie nie dotyczy, może sprawić, że stracimy czujność.

Prowadzący: Jak nie dać się zmanipulować? O jakich zasadach warto pamiętać?

Joanna Rudzińska-Wojciechowska: Warto zwrócić uwagę na odczucia płynące z ciała. Jeśli zaczniemy czuć silne pobudzenie, spięcie mięśni czy szybsze bicie serca, to może być znak, że padamy ofiarą manipulacji. Warto wtedy zatrzymać się, wziąć kilka głębokich wdechów i spojrzeć na sytuację z dystansu. Taka chwila refleksji pozwala odzyskać kontakt z naszym racjonalnym „ja”. Weryfikowanie informacji nie jest wyrazem braku zaufania – to naturalna i rozsądna reakcja. Jeśli ktoś utrudnia nam potwierdzenie faktów, to wyraźny sygnał, że coś jest nie tak.

Odcinek 6. Gość – Anna Bichta

Prowadzący: Co dwie głowy, to nie jedna. Dziś sprawdzamy, dlaczego o bezpieczeństwo cyfrowe lepiej dbać razem. O tym, jak dzielenie się wiedzą z bliskimi zwiększa naszą odporność na oszustwa w sieci, opowiada Anna Bichta z fundacji THINK!. Na jakie „bezpieczniki” warto umówić się z bliskimi?

Anna Bichta: Jednym z bezpieczników może być rodzinne hasło – znane tylko nam i naszym najbliższym. To może być data urodzenia pupila, słowo kojarzące się z wakacjami sprzed lat albo wyraz, który nasze dziecko lubiło powtarzać w dzieciństwie. Takie proste rozwiązanie pomoże chronić się przed oszustwem „na bliską osobę". Jeśli otrzymamy podejrzany telefon, możemy zapytać o to hasło. Jeśli rozmówca się zawaha lub go nie zna, należy się po prostu rozłączyć.

Prowadzący: Dlaczego rozmowa z bliskimi to skuteczne lekarstwo na cyberoszustwa?

Anna Bichta: Podobnie jak w medycynie, w bezpieczeństwie cyfrowym lepiej zapobiegać niż leczyć. Profilaktyka, czyli edukacja i rozmowy, utrudnia pracę oszustom. Przestępcy liczą na naszą izolację i to, że nie skonsultujemy podejrzanej sytuacji z nikim innym. Dzielenie się historiami usłyszanymi w mediach czy poradami to tarcza chroniąca nasze pieniądze.

Prowadzący: Jakie jeszcze zasady warto wdrożyć?

Anna Bichta: Warto przygotować wspólną listę kontaktów do osób i instytucji, które pomogą w razie problemów. Dobrze jest też przyjąć zasadę konsultowania każdej decyzji finansowej powyżej pewnej kwoty (np. 100 zł) z bliskimi i odczekania jednego dnia przed jej podjęciem. Warto także ustawiać limity dzienne na koncie bankowym. Zapraszam na stronę bezpiecznezlotowki.pl, gdzie opisujemy techniki oszustów i historie osób, na których można się wiele nauczyć.

Ministerstwo Finansów
FUNDUSZ EDUKACJI FINANSOWEJ
think!
FUNDACJA ROZWOJU SPOŁECZEŃSTWA WIEDZY

Sfinansowano ze środków Funduszu Edukacji Finansowej, którego dysponentem jest Minister Finansów i Gospodarki. Realizatorem Kampanii jest Fundacja Think!